

## PERLINDUNGAN HUKUM TERHADAP KONSUMEN KARTU SIM YANG MENGALAMI KEBOCORAN DATA AKIBAT PERETASAN

Fadhi Khoiru Nasrudin<sup>1</sup>, Rosalinda Elsin Latumahina<sup>2</sup>

<sup>1,2</sup>Fakultas Hukum, Universitas 17 Agustus 1945 Surabaya

Email: [d.ganzz@yahoo.com](mailto:d.ganzz@yahoo.com), [rosalindael@untag-sby.ac.id](mailto:rosalindael@untag-sby.ac.id)

### Abstract

*The development of the internet cannot be separated from the development of the concept of personal data. Information technology today has developed very quickly and rapidly. This is because information technology is able to eliminate the boundaries of space, distance and time so as to significantly increase aspects of productivity and efficiency. The presence of digital crime has developed into a threat to human life, making it difficult for public authorities to know the strategies for violations committed with computer innovation, especially internet networks. So the main problem in this research is whether the Personal Data Protection Law can protect SIM card consumers against hacking of personal data? Data protection is a term that is often used to refer to binding practices, safeguards and rules put in place to protect personal data and ensure that the data subject remains in control. Article 12 paragraph (1) Personal Data Subjects have the right to sue and receive compensation for violations of processing Personal Data about themselves in accordance with statutory provisions. The approach to this problem is to use a method that reviews the regulations and provisions that have been in force and are often followed by the community. Therefore, the type of research used includes normative legal research.*

**Keywords :** Law, Protection, Technology

### Abstrak

Perkembangan internet tidak lepas dari perkembangan konsep data pribadi. Teknologi informasi pada zaman sekarang telah berkembang sangat cepat dan pesat. Hal ini disebabkan karena teknologi informasi mampu menghapus batas ruang, jarak serta waktu sehingga dapat meningkatkan aspek produktivitas dan efisiensi secara signifikan. Kehadiran kejahatan digital telah berkembang menjadi ancaman bagi kehidupan manusia sehingga sulit bagi otoritas publik untuk mengetahui strategi pelanggaran yang dilakukan dengan inovasi komputer terutama jaringan internet. Maka yang menjadi pokok permasalahan dalam penelitian ini yaitu Bagaimanakah Undang-Undang Perlindungan Data Pribadi dapat melindungi konsumen kartu SIM terhadap peretasan data pribadi? Perlindungan data adalah istilah yang sering digunakan untuk merujuk pada praktik, perlindungan, dan aturan yang mengikat yang diberlakukan untuk melindungi data pribadi dan memastikan bahwa subjek data tetap memegang kendali. Landasan hukum yang dapat dijadikan sebagai tumpuan untuk mengajukan tuntutan apabila terjadinya kebocoran data akibat peretasan adalah Pasal 12 ayat (1) Subjek Data Pribadi berhak menggugat dan menerima ganti rugi atas pelanggaran pemrosesan Data Pribadi tentang dirinya sesuai dengan ketentuan perundang-undangan. Pendekatan terhadap masalah ini adalah dengan menggunakan metode yang meninjau ketentuan aturan yang telah berlaku dan sering diikuti oleh masyarakat. Oleh karena itu, jenis penelitian yakni yang digunakan termasuk penelitian hukum normatif.

**Kata Kunci :** Hukum, Perlindungan, Teknologi

## PENDAHULUAN

Perkembangan internet tidak lepas dari perkembangan konsep data pribadi. Teknologi informasi pada zaman sekarang telah berkembang sangat cepat dan pesat. Namun, setiap kelebihan pasti akan ada kekurangan terutama pada perkembangan teknologi informasi tersebut bagi pengguna teknologi tersebut. Perkembangan zaman demi zaman telah memberikan peranan penting bagi berkehidupan bermasyarakat. Hal ini disebabkan karena Inovasi data dapat menghapus batasan ruang, jarak, dan waktu untuk secara esensial membangun efisiensi dan sudut pandang kecakapan.

Dalam masyarakat saat ini, kemajuan teknologi komunikasi informasi berbasis komputer telah meningkat pesat. Kemudian, perkembangan teknologi ini sangat membantu masyarakat. Masyarakat memandang keberadaan internet sebagai teknologi yang bermanfaat untuk kehidupan. Pemanfaatan internet dalam berbagai bidang kehidupan tidak hanya memudahkan berbagai hal, tetapi juga mengungkap sejumlah persoalan, termasuk persoalan hukum. Pengamanan informasi seseorang (*the protection of privacy rights*) merupakan salah satu potensi masalah hukum.

Faktanya, belum adanya perangkat hukum yang secara khusus menjawab kebutuhan masyarakat akan perlindungan privasi, konsumen di Indonesia masih kekurangan kepastian dan perlindungan atas data pribadi dan privasinya dan data pribadi yang lebih kuat. Bisa berakibat fatal bahkan menjadi ancaman bagi masyarakat jika hukum Indonesia tidak mengantisipasi perubahan teknologi informasi.

Metode pengumpulan data yang masif muncul sebagai hasil dari kemajuan teknologi yang ditujukan untuk memenuhi kebutuhan kehidupan manusia modern di era digital. Ketika pihak-pihak ini mengumpulkan data tanpa jaminan perlindungan hukum, mereka cenderung bertindak sewenang-wenang dan menyalahgunakan data yang dikumpulkan. Karena sejumlah besar bisnis swasta yang beroperasi di berbagai industri, termasuk Informasi pribadi pengguna dikumpulkan oleh asuransi, perbankan, telekomunikasi, dan penyedia layanan transportasi online, Indonesia perlu mengadopsi peraturan hukum yang mendesak untuk perlindungan data pribadi. Sebagai pengelola data, perusahaan berkewajiban untuk melindungi data konsumen dari pencurian dan kebocoran.

Seiring dengan pesatnya kemajuan teknologi internet, kejahatan dunia maya dikenal dengan *cybercrime* baru bermunculan via jaringan internet. Di Indonesia telah terjadi beberapa kejadian antara lain peretasan, penipuan, *email spamming*, pengolahan data menggunakan program komputer untuk mengakses data orang lain dan penyadapan data mereka.

*Cybercrime* yang juga dikenal sebagai kejahatan dunia maya telah berkembang menjadi ancaman serius bagi kehidupan manusia sehingga sulit bagi pemerintah untuk mengikuti strategi yang digunakan dalam kejahatan yang berhubungan dengan komputer, terutama yang melibatkan jaringan terutama internet. Hal tersebut merupakan efek dari perkembangan terhadap teknologi informasi, yang memiliki dampak positif ataupun negatif dalam segala hal. Salah satu hasilnya adalah kepemilikan data dan informasi pribadi..

Meningkatnya kasus kejahatan kebocoran data pribadi akibat peretasan yang memanfaatkan teknologi informasi yang teridentifikasi pada tahun 2022, dengan contoh kasus kebocoran data pengguna aplikasi e-HAC KeMenKes, kebocoran data NIK pengguna nomor telpon, kebocoran data BPJS Kesehatan, kebocoran data nasabah BRI Life, kebocoran data DPT pemilu KPU, kebocoran data pengguna Tokopedia, sertifikat vaksin Presiden RI, data pribadi situs media sosial seperti Instagram dan Facebook, data indiHome dan masih banyak yang lainnya. Selain itu, pengelolaan informasi data khususnya pengelolaan data pribadi, merupakan salah satu peluang kejahatan dalam perkembangan teknologi informasi. Karena berbagai data informasi pribadi tidak sukar untuk diakses sehingga diperlukannya perlindungan data pribadi. Batasan privasi semakin tipis akibat kemajuan teknologi informasi dan komunikasi.

Dengan mengirimkan Nomor Induk Kependudukan (NIK) dan Nomor Kartu Keluarga (KK) melalui pesan singkat, pengguna kartu prabayar seluler harus mendaftarkan informasi pribadinya, yang kemudian disinkronkan dengan data dari Ditjen Kemendagri Kependudukan Catatan Sipil.

Secara teknis, pemerintah mengumpulkan data registrasi kartu SIM, namun pesan pelanggan terlebih dahulu masuk ke SMS milik provider. Proses penguncian data ini berisiko karena tidak ada cara untuk memastikan bahwa informasi pribadi pelanggan dilindungi dan dirahasiakan. Permenkominfo Nomor 20 Tahun 2016 Tentang Perlindungan Data Pribadi

Dalam Sistem Elektronik (selanjutnya disebut Permenkominfo PDPSE) telah berusaha untuk melindungi hak atas privasi, tetapi tidak ada peraturan keamanan lengkap untuk privasi data, dengan mengumpulkan informasi pribadi rentan disalahgunakan. Selain itu, pencurian data pribadi tidak menghasilkan sanksi atau pemulihan..

Pasal 1365 KUHPPerdata pada dasarnya menjelaskan bahwa segala tindakan hukum yang merugikan orang lain, kemudian individu menimbulkan kerugian itu harus diberi ganti rugi dan Pasal 12 ayat (1) UU PDP Subjek Data Pribadi berhak menggugat dan menerima ganti rugi atas pelanggaran pemrosesan Data Pribadi tentang dirinya sesuai dengan ketentuan perundang-undangan yang merupakan dasar hukum yang dapat dijadikan sebagai dasar pengajuan gugatan atas kebocoran data akibat peretasan. kesalahan/kelalaian adalah aturan tanggung jawab yang bersifat emosional, yang berarti bahwa gagasan kewajiban ini muncul tergantung pada cara berperilaku pelaku bisnis/pembuat yang bersangkutan.

Pengaturan ini didasarkan pada prinsip-prinsip hukum yang ditetapkan, dan setiap pelanggan memiliki hak untuk menuntut. Proses pengadilan berlangsung lama, dan konsumen harus melakukan proses penetapan kerugian akibat kebocoran data pribadi selama masa percobaan dan penetapan kelalaian atau kesalahan yang menyebabkan kebocoran tersebut. Tidak ada undang-undang khusus mengenai keamanan data pribadi yang menentang tuntutan konsumen atas pertanggungjawaban individu jika terjadi kebocoran data pribadi.

Istilah "perlindungan data" umumnya mengacu pada prosedur yang mengikat, pengamanan, dan aturan yang berlaku untuk tetap mengontrol subjek data dan melindungi data pribadi. Intinya, pemilik data harus dapat memilih apakah akan membagikan data tertentu ataupun tidak, serta siapa saja yang dapat mengaksesnya, untuk seberapa lama, dan untuk tujuan apa.

Pada jurnal dengan judul "Perlindungan Hukum Terhadap Konsumen Kartu Sim Dan NIK Yang Mengalami Kebocoran Data Akibat Peretasan" membahas dasar hukum yang dijadikan sebagai landasan untuk mengajukan gugatan apabila terjadi kebocoran data pribadi akibat peretasan yaitu Pasal 12 ayat (1) Subjek Data Pribadi berhak menggugat dan menerima ganti rugi atas pelanggaran pemrosesan Data Pribadi tentang dirinya sesuai dengan ketentuan perundang-undangan. Kesalahan merupakan asas tanggungan yang bersifat subyektif, artinya

Kewajiban ini timbul dari perbuatan pelaku usaha atau produsen yang bersangkutan. Mengajukan gugatan jika terjadi kebocoran data pribadi akibat peretasan.. Sedangkan pada jurnal dengan judul “Upaya Perlindungan Hukum Bagi Konsumen Ditinjau Dari Undang-Undang Perlindungan Konsumen” membahas perlindungan hukum bagi pelanggan diatur oleh Undang-Undang Perlindungan Konsumen maka pelaku usaha harus memberikan perlindungan hukum kepada konsumen. Selain itu, dalam hal terjadi perselisihan, upaya hukum untuk menyelesaikannya dapat melibatkan penyelesaian perselisihan litigasi atau non-litigasi. penyelesaian melalui litigasi berdasarkan tuntutan salah satu pihak. Negosiasi, konsiliasi, mediasi, dan arbitrase adalah contoh metode penyelesaian sengketa non-litigasi.

Pada jurnal dengan judul “Perlindungan hukum terhadap nasabah yang mengalami kerugian akibat peretasan kartu kredit” membahas tentang bank sebagai pelaku usaha bertanggung jawab untuk mengganti kerugian nasabah yang dideritanya sebagai konsumen. apabila nasabah mengalami kesusahan finansial akibat skimming di perbankan yang bukan milik nasabah. Skimming menyebabkan pelanggan kehilangan semua uang mereka, yang merupakan kerugian. Apabila nasabah mengalami kerugian akibat skimming di industri perbankan, maka dapat dilakukan tindakan sebagai berikut: dapat mengajukan pengaduan kepada bank yang bersangkutan, selain itu bank berkewajiban untuk menyelidiki dan menanggapi setiap dan semua keluhan nasabah. Namun, nasabah memiliki pilihan untuk memilih penyelesaian yang berbeda jika penyelesaian bank masih belum memuaskan, seperti melalui Badan Penyelesaian Lembaga Konsumen dan pengadilan, mediasi perbankan, atau negosiasi.

Pada jurnal dengan judul “Perlindungan Hukum Terhadap Data Pribadi Konsumen Yang Diredas Berdasarkan Peraturan Menteri Komunikasi Dan Informatika Nomor 20 Tahun 2016 Tentang Perlindungan Data Pribadi Dalam Sistem Elektronik” membahas tentang Peraturan Menteri Komunikasi dan Informatika No.20 Tahun 2016, akan tetapi pengamanan sah yang bersifat abusive dalam pedoman ini belum dapat memberikan jaminan yang memadai karena belum adanya kewenangan yang memadai untuk mengurangi atau menghentikan oknum penjahat pelanggar informasi. Perlindungan hukum atas informasi pribadi pelanggan adalah tanggung jawab perusahaan yang menjalankan sistem elektronik jika data pribadi pelanggannya diretas. Ketika konsumen menerima persyaratan layanan yang ditawarkan oleh

perusahaan yang mengoperasikan sistem elektronik, hak dan tanggung jawab dibuat antara perusahaan yang mengoperasikan sistem elektronik dan konsumen. Dengan begitu telah ada komitmen yang terjadi di antara pertemuan-pertemuan itu. Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi menetapkan sanksi hukum terhadap individu yang melakukan pelanggaran peretasan data pribadi.

Berdasarkan latar belakang di atas, maka dipilih judul tentang “Perlindungan Hukum Terhadap Konsumen Kartu SIM yang Mengalami Kebocoran Akibat Peretasan”.

## METODE PENELITIAN

### a. Jenis Penelitian

Pendekatan terhadap masalah ini adalah dengan menggunakan metode yang meninjau ketentuan peraturan dan undang-undang yang ada dan diterima oleh masyarakat pada umumnya (Soekanto, 2007). Sehingga penelitian normatif legislatif digunakan dalam jenis penelitian ini.

### b. Metode Pendekatan

Teknik metodologi yang digunakan adalah metodologi melalui pedoman hukum (statue approach) dan pendekatan berorientasi konteks (conceptual approach), yang berpusat pada pengaturan peraturan dan pedoman yang telah ditetapkan. Sumber hukum primer, sumber data sekunder, dan sumber data tersier yang dikumpulkan dari bahan pustaka menjadi dasar sumber data penelitian ini.

### c. Sumber dan jenis bahan hukum

- Bahan hukum primer berupa ketentuan Undang-Undang.
- UUD RI Tahun, 1945.
- UU. No. 36 Tahun, 1999 mengenai Telekomunikasi.
- UU No., 19 Tahun, 2016 mengenai Perubahan, atas UU No. 11, Tahun 2008 mengenai Informasi dan Transaksi, Elektronik, (selanjutnya disebut UU ITE).
- UU. No. 8, Tahun 1999 mengenai, Perlindungan, Konsumen.
- UU No., 39 Tahun 1999 mengenai, HAM (Hak Asasi Manusia).
- UU, No. 24, Tahun 2013 mengenai, Administrasi Pemerintahan.
- UU No. 14 Tahun, 2008 mengenai, Keterbukaan Informasi, Publik.

- UU Perlindungan Data Pribadi
- Peraturan Menteri No. 20 Tahun 2016 Tentang Perlindungan Data Elektronik Sistem Privat.
- Peraturan Menteri No. 82 tahun 2012 mengenai Penyelenggaraan Sistem dan Informasi Elektronik.
- Peraturan Menteri Komunikasi, Dan Informatika, No. 21 Tahun 2017 mengenai Perubahan Kedua atas Peraturan Menkominfo, No. 12 Tahun 2016 tentang Registrasi Pelanggan, Jasa Telekomunikasi
- Kajian ini menggunakan bahan hukum sekunder seperti pendapat ahli dalam buku, jurnal, dan website serta pendapat hukum tentang bagaimana melindungi warga negara dengan NIK yang telah dibocorkan datanya oleh hacker.
- Bahan hukum tersier dalam penelitian, ini meliputi kamus hukum, yang mengenai tentang, Perlindungan, Hukum terhadap pengguna, kartu SIM dan NIK yang Mengalami Kebocoran, Data akibat, peretasan.
- d. Teknik pengumpulan bahan hukum
  - Menggunakan teknik inventarisasi dan kategorisasi, bahan hukum utama terdiri dari peraturan.
  - Sistem kartu catatan (card system) digunakan untuk mengumpulkan bahan hukum sekunder. Bahan-bahan tersebut meliputi kartu rangkuman, kartu kutipan, dan kartu ulasan yang masing-masing berisi analisis dan catatan khusus penulis serta garis besar dan gagasan utama yang berisi pendapat orisinal penulis.
- e. Teknik analisis bahan hukum
  - Melalui penangkapan, harmonisasi, sistematisasi, dan penemuan hukum, teknik analisis yang digunakan adalah preskriptif.

## HASIL PENELITIAN DAN PEMBAHASAN

### 1. Konsep data pribadi dan privasi

Yang dimaksud dengan data bersifat pribadi yaitu data yang terkait identitas, simbol, kode, angka atau huruf penanda atas seseorang yang bersifat rahasia dan pribadi. Nama,

karakteristik, usia, pendidikan, jenis kelamin, pekerjaan, dan posisi keluarga adalah contoh informasi data pribadi. Salah satu identitas data pribadi tersebut tercantum dalam KTP.

Berdasarkan research terbukti bahwa istilah "perlindungan data" pertama kali digunakan pada tahun 1970-an di Swedia dan Jerman yang memberlakukan aturan terhadap perlindungan data pribadi menjadi undang-undang dan peraturan yang sistematis untuk mengatur perlindungan data pribadi.

Regulasi informasi seseorang atau pribadi diberlakukan karena saat ini digunakan suatu perangkat teknologi untuk mengumpulkan data sensus pada saat digunakan untuk menyimpan data kependudukan, peraturan data harus ditegakkan. Namun kenyataannya, pemerintah atau swasta tetap melakukan berbagai pelanggaran. Istilah "data pribadi" dan "informasi pribadi" didefinisikan secara berbeda di setiap negara. Namun, dari sudut pandang substantif, ke2 istilah tersebut sering digunakan secara berganti karena definisinya yang hampir identik. Dalam undang-undang ITE mereka, Malaysia dan Indonesia, serta negara di UE atau Uni Eropa, menggunakan istilah "data pribadi", sedangkan Australia, Kanada, dan Amerika Serikat menggunakan istilah "informasi pribadi".

Di dalam data pribadi termasuk informasi, komunikasi, atau pendapat tentang informasi rahasia, pribadi, atau sensitif seseorang yang ingin dicegah oleh orang lain untuk menggunakan, mengumpulkan, atau membagikannya.

Latumahina mengartikan data pribadi sebagai informasi yang berkaitan tentang individu dan dapat dibedakan satu sama lain. Atas dasar prinsip ini, perlindungan informasi pribadi terbagi menjadi 2 jenis: jenis perlindungan data fisik, yang mencakup data yang terlihat dan tidak terlihat, dan jenis kedua, yang mencakup pengaturan menggunakan informasi data individu yang tidak menyusunnya, jaminan data untuk tujuan tersebut, dan pemusnahan data itu sendiri.

## **2. Asas keamanan data individu**

UU mengenai Perlindungan Data Pribadi dilaksanakan berdasarkan atas asas perlindungan, asas kepentingan umum, asas keseimbangan dan asas pertanggungjawaban (Berdasarkan Pasal 2 UU PDP)

- a. "Prinsip Perlindungan" mengatur bahwa pemerintah harus memberikan perlindungan data pribadi di dalam dan di luar kepada warganya.



- b. "Prinsip Kepentingan Umum" mengacu pada struktur perlindungan kepentingan umum Konstitusi yang luas.
- c. "Prinsip keseimbangan" mengacu pada keseimbangan antara hak privasi dan kewajiban hukum negara untuk melayani kepentingan publik.
- d. "Prinsip Akuntabilitas" menetapkan bahwa pengelola data harus bertanggung jawab untuk memelihara data pribadi.

Data pribadi harus dijaga karena banyak kejahatan yang dilakukan di era digital saat ini. Namun, banyak masyarakat Indonesia yang tidak menyadari pentingnya kerahasiaan data pribadi dan seringnya terjadi penyalahgunaan data pribadi oleh pihak-pihak yang pasti tidak bertanggung jawab.

Maka tantangan sebagai konsumen platform via digital sebaiknya bisa melakukan upaya perlindungan terhadap data diri kita sendiri ataupun orang lain. Masyarakat Indonesia gemar berbagi serta berinteraksi sehingga kita lupa bahwa ada orang tidak bertanggungjawab atau pihak yang memanfaatkan data diri kita.

Lemahnya keamanan informasi individu di Indonesia telah menimbulkan kebocoran informasi yang luas. dicontohkan dengan maraknya kasus kejahatan di dunia online, contohnya kasus *hacking* dan pembajakan media sosial yang mengakibatkan bocornya sebuah data, penipuan, bahkan pemerasan di media online.

Dalam konteks saat ini, data pribadi merupakan *the new oil*. Terlebih kita pasti memberikan informasi data dan nama secara lengkap serta nomor telepon genggam. Di sisi waktu lain, terkadang kita memberikan informasi data alamat rumah atau alamat e-mail. Gabungan informasi data tersebut dapat disalahgunakan fungsinya oleh pihak-pihak yang tidak bertanggung jawab, misalnya untuk kepentingan pribadi atau bisa disebut(*scam*).

Pemerintah juga mengakui tekanan untuk menerapkan sejumlah peraturan penting untuk melindungi data pribadi. Faktanya, pemerintah Indonesia telah memberlakukan sejumlah peraturan dan regulasi perlindungan data pribadi, meskipun masih bersifat umum. Misalnya, Peraturan No. 20 Tahun 2016 mengenai Sistem Elektronik dan Pengamanan Data Pribadi yang dikeluarkan oleh Menteri Komunikasi Informatika dapat digunakan mulai dari Desember 2016.

Melindungi data atau informasi pribadi seseorang dapat dimulai dari diri sendiri. Mirip dengan banyak apps, terutama untuk media sosial, banyak di antaranya menawarkan kode cadangan, verifikasi dua langkah, dan bahkan pemberitahuan email jika pihak ketiga mencoba masuk atau mengakses akun media sosial pribadi kita.

Sejumlah metode untuk menjaga data pribadi, antara lain:

Beliau juga memberikan sejumlah metode untuk menjaga data pribadi, antara lain:

1. Ketika mengelola perangkat lunak pada perangkat teknologi, khususnya kata sandi, kita harus cerdas dan rajin;
2. memaksimalkan keamanan informasi pribadi, seperti dengan menjual email untuk digunakan dalam bisnis dan aktivitas lainnya atau dengan menghubungkan keuangan kami (mbanking);
3. Persiapkan penipuan digital dengan membaca lebih banyak buku dan postingan media sosial tentang metode penipuan digital baru;
4. menyatukan rekam jejak digital kami sekaligus menjaga privasi kehidupan pribadi kami; dan Harmony, yang bekerja sama untuk melindungi data pribadi sambil selalu waspada di zaman sekarang ini ketika jejak digital dapat bertahan lebih lama dari masa hidup kita.

Perlu diingat bahwa data pribadi setiap individu itu privasi. maka dengan itu, kita harus menjaga dan melindungi data pribadi satu sama lain dan tidak mengizinkan pihak-pihak yang tidak bertanggungjawab untuk mengakses informasi setiap individu.

Data yang terkait dengan individu atau "data pribadi" adalah informasi yang dapat diidentifikasi secara baik dengan sendirinya atau ketika digabungkan dengan informasi lain, baik secara langsung maupun tidak langsung melalui sistem elektronik dan non-elektronik.

Bahwa meski Undang-Undang Perlindungan Data Pribadi sudah disahkan, peretas akan tetap eksis dan beraksi. Akan selalu ada peretas, apa pun hukumnya. Badan Siber dan Sandi Negara (BSSN) masih berperan penting dalam menjaga dunia maya Indonesia sebagai salah satu kunci terpenting keamanan data yaitu bagaimana menggunakan enkripsi lalu lintas data yang kuat.

Diharapkan Badan Siber dan Sandi Negara (BSSN) dapat menetapkan prosedur keamanan data standar yang harus dipatuhi oleh semua perusahaan manajemen data, memperkuat posisinya, dan meningkatkan kapabilitasnya di bidang sumber daya manusia (SDM).

Diharapkan lembaga perlindungan data pribadi (PDP), Badan Siber dan Sandi Negara (BSSN) serta Kemenkominfo bisa bahu membahu menjalankan fungsinya dengan baik sempurna sesuai tupoksinya, tuk menciptakan ranah *cyber* yang bersifat aman, sehat dan juga bermanfaat bagi masyarakat Indonesia.

Adanya UU PDP juga diharapkan bisa mengurangi bahkan mencegah resiko atau terjadinya kebocoran terkait data dikarenakan ancaman berupa sanksi yang jelas bagi pihak pengelola data. Namun, kehadiran undang-undang Keamanan Informasi Pribadi tidak akan langsung mengurangi peretasan karena UU PDP sudah diretas oleh programmer yang melanggar hukum dan bisa sangat ditegur oleh kesalahan langkah mereka tanpa Peraturan PDP.

Dengan berlakunya UU PDP terbaru ini berharap justru kepada pengelola data dapat lebih peduli dan lebih baik tentang mengelola data-data dan inti penting dari hal ini berada di pihak lembaga yang akan dibentuk untuk mengawasi peran serta pengelolaan data pribadi tersebut. Jika dapat menjalankan tugasnya dengan sangat baik dan berkomunikasi dengan sempurna institusi pengelola data yang berada di bawah pengawasannya dan bertaji selevel satgas pengendali kebocoran data yang akan dibentuk Menkopolhukam, maka hal tersebut akan memberi pengaruh yang sangat signifikan kepada perbaikan pada pengelolaan data di bangsa Indonesia. Tetapi kalau tidak, maka tidak dapat memberikan efek signifikan kepada perbaikan sistem pengelolaan data di bangsa Indonesia.

Masalah keamanan data pribadi dan keamanan sistem informasi saat ini menjadi salah satu masalah paling mendasar yang mempengaruhi transaksi online dan elektronik.

## KESIMPULAN

Undang-Undang Perlindungan Data Pribadi sudah diterapkan dan disahkan pada tahun 2022. Dengan adanya aturan atau peraturan yang secara khusus melindungi data pribadi atau tiap data privasi yang dimiliki oleh masyarakat Indonesia, menjadikan perlindungan data pribadi telah diatur secara menyeluruh. Tetapi dengan adanya peraturan perundang-undangan yang mengatur data pribadi, tidak memastikan atau tidak menjamin kejadian

*cybercrime* tersebut terulang kembali khususnya kebocoran data yang berakibat Undang-Undang Perlindungan Data Pribadi disahkan secara langsung. Maka diperlukan sumber daya manusia (SDM) yang seimbang dengan peraturan perundang-undangan yang mengatur secara kuat dan menyeluruh. Tanpa hadirnya sumber daya manusia (SDM) yang seimbang maka sebuah Undang-Undang Perlindungan Data Pribadi (UU PDP) hanyalah sebuah peraturan yang membahas bagaimana jika terjadi sebuah *cybercrime* yang terjadi kepada bangsa Indonesia khususnya masyarakat Indonesia yang mengalami kerugian akibatnya kebocoran data tersebut.

#### DAFTAR PUSTAKA

- Benuf, K. (2020). URGENSI KEBIJAKAN PERLINDUNGAN HUKUM TERHADAP KONSUMEN FINTECH PEER TO PEER LENDING AKIBAT PENYEBARAN COVID-19. *Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional*, 9(2). <https://doi.org/10.33331/rechtsvinding.v9i2.427>
- Carundeng, R. B., Wahongan, A. S., & Prayogo, P. (2022). Perlindungan Hukum Terhadap Data Pribadi Konsumen Yang Diretas Berdasarkan Peraturan Menteri Komunikasi Dan Informatika Nomor 20 Tahun 2016 Tentang Perlindungan Data Pribadi Dalam Sistem Elektronik. *Lex Privatum*, X(1), 188–198.
- Chen, E., Afif, M. I., Jason, W., Sidauruk, C. F., & Anugrah, S. P. (2021). Perlindungan Hukum Terhadap Konsumen Pengguna Pinjaman Online Illegal. *Prosiding Serina*, 1(1), 2045–2052. <https://doi.org/10.24912/pserina.v1i1.18080>
- Dairobby, W. A. (2020). *Perlindungan Hukum Terhadap Penyalahgunaan Data Pribadi Dalam Layanan Transportasi Berbasis Aplikasi Online*. <http://repository.uir.ac.id/id/eprint/9721>
- de la Tierra, A. (2017). Con Men. *Sociological Forum*, 32(3), 684–686. <https://doi.org/10.1111/socf.12355>
- Dewi Rosadi, S., & Gumelar Pratama, G. (2018). URGENSI PERLINDUNGANDATA PRIVASIDALAM ERA EKONOMI DIGITAL DI INDONESIA. *Veritas et Justitia*, 4(1), 88–110. <https://doi.org/10.25123/vej.2916>
- Kusnadi, S. A. (2021). Perlindungan Hukum Data Pribadi Sebagai Hak Privasi. *AL WASATH Jurnal Ilmu Hukum*, 2(1), 9–16. <https://doi.org/10.47776/alwasath.v2i1.127>
- Novita, Y. D., & Santoso, B. (2021). Urgensi Pembaharuan Regulasi Perlindungan Konsumen di Era Bisnis Digital. *Jurnal Pembangunan Hukum Indonesia*, 3(1).
- Priscyllia, F. (2019). Perlindungan Privasi Data Pribadi dalam Perspektif Perbandingan Hukum. *Jatiswara*, 34(3), 1–5. <https://doi.org/10.29303/jatiswara.v34i3.218>
- Rahmatullah, I. (2021). Pentingnya Perlindungan Data Pribadi Dalam Masa Pandemi Covid-19 Di Indonesia. *'Adalah*, 5(1), 11–16. <https://doi.org/10.15408/adalah.v5i1.19811>
- Saadah, K. A. W. (2020). Jurnal Ilmiah Pendidikan Pancasila dan Kewarganegaraan. *Jurnal: Pendidikan Pancasila Dan Kewarganegaraan*, Volume 5(Nomor 1), hlm: 131-138. <http://journal2.um.ac.id/index.php/jppk/article/view/7820/3749>
- Satrio, M. B., & Widiatno, M. W. (2020). Perlindungan Hukum Terhadap Data Pribadi Dalam Media Elektronik (Analisis Kasus Kebocoran Data Pengguna Facebook Di Indonesia). *JCA of*

- Law*, 1(1), 49–61. <https://jca.esaunggul.ac.id/index.php/law/article/view/6>
- Sautunnida, L. (2018). Urgensi Undang-Undang Perlindungan Data Pribadi di Indonesia: Studi Perbandingan Hukum Inggris dan Malaysia. *Kanun Jurnal Ilmu Hukum*, 20(2), 369–384. <https://doi.org/10.24815/kanun.v20i2.11159>
- Yudhi Priyo Amboro, F., & Puspita, V. (2021). Perlindungan Hukum Atas Data Pribadi (Studi Perbandingan Hukum Indonesia dan Norwegia) | CoMBInES - Conference on Management, Business, Innovation, Education and Social Sciences. *CoMBInES*, 1(1), 415–427. <https://journal.uib.ac.id/index.php/combines/article/view/4466>
- Yuniarti, S. (2019). Perlindungan Hukum Data Pribadi Di Indonesia. *Business Economic, Communication, and Social Sciences (BECOSS) Journal*, 1(1), 147–154. <https://doi.org/10.21512/becossjournal.v1i1.6030>